

# The integration of security systems



*Safeguarding your security*

## The integration of security systems

From time to time, it is useful to refresh the memory, in particular with respect to security issues. They say we should learn from history in order to avoid past mistakes, and February 2006 saw the 10th anniversary of an attack with a curious name: Smurfing. No doubt many of you who are reading this will remember the Smurfs, the little blue creatures created by Peyo, the Belgian cartoonist.

A smurfing attack consists of sending large quantities of pings to the network broadcast IP address, all of them with a false IP address: that of the victim. If the router allows it, all network systems will respond to the ping, multiplying the traffic and saturating the victim's computer to the point in which it may cease to respond.

Evidently, today this type of attack is considered almost extinct, as any corporate network (no matter how small) has a firewall which, almost certainly, prevents replies to external pings therefore neutralizing this type of attack. However, there are many other ways of launching an attack without resorting to smurfs, and there are plenty of examples to underline this.

One clear example is the SQLSlammer worm. This worm multiplied itself through an instruction given through port 1434. This port is used for communication between different SQL Servers when they need to share information, and so in some cases it was necessary for it to be open. But in many other cases (such as those in which components of SQL Server, for example SQL Server clients, were installed) this port was open unnecessarily.

Nowadays both port 7 and port 1434 are normally closed, as are many others. Generally, the ports left open are those that are strictly necessary for a company or organization to operate. Nevertheless, who's to say that these ports aren't susceptible to threats?

The solution involves monitoring the applications that use the open ports in companies in order to identify abnormal behavior and when problems are detected, shut down the communication. Today however, the solutions that can offer the necessary information to secure the system are spread out across different network devices.

On the one hand, HIPS (Host-based Intrusion Prevention Systems) are normally installed on computers that are not in the first line of the connection. They could be in an internal server or client computer, preferably in the DMZ, but not in the same connection port. This point is usually covered by the firewall, a static system with settings pre-programmed by the network administrator or even by an external security provider, but this is independent of other protection systems.

Levels of security now demanded by network administrators require a reaction speed the current security model cannot offer. The time that passes between a system detecting an intrusion and the administrator deciding to close the corresponding port in the firewall could be too long and have disastrous consequences. We are not talking here about hours, but about less than it takes for

# The integration of security systems



*Safeguarding your security*

the administrator to enter his passwords and enter the security system administration console: simply seconds.

The solution involves integrating devices to combine all technologies in a single system. A firewall is very useful but it needs continuous rule updates, an HIPS does not protect against unknown threats. However, the integration of the two solutions could be the answer to the current threat scenario. And not just the HIPS and the firewall, but the integration of applications should also include a traditional antivirus, able to detect other types of threats such as, spyware, spam, phishing...

The current security situation requires a new orientation security of systems. The creators of malware have taken an important step toward their objectives and it is not just our information that is at risk, but also our money. Access to IT systems by hackers is no longer simply destructive, as now there is an added incentive to penetrate corporate networks: money.

Moreover, there are now attacks that target specific systems, and so there is a need for all security tools be concentrated in a single point of the network: the Internet entry point. If the protection is further back or spread across different points, the defensive response may not be effective enough.

Unification of protection in a place as critical as the Internet entry point opens the way for the concept of prevention against all types of attacks and intrusions at global network level. This concept is called NIPS (Network Intrusion Prevention System) and is the best guarantee today for implementing effective network protection.